Weaver Trust
Inspire - Believe - Achieve

1. Scope and Purpose

1.1 Weaver Trust's IT and communications systems are intended to promote effective communication and working practices within the Trust. This policy outlines the standards staff must observe when using these systems, the circumstances in which the Trust will monitor their use, and the action the Trust will take in respect of breaches of these standards.

1.2 In particular, remember that staff are representatives of the Trust and all communication through our systems (whether by telephone, e-mail or otherwise), must be conducted in an appropriate manner.

1.3 This policy does not form part of any employee's contract of employment and may be amended at any time.

1.4 This policy deals mainly with the use (and misuse) of computer equipment, e-mail, the internet, telephones, mobile telephones, tablets, personal digital assistants (PDAs) and voicemail. It also applies to the use of fax machines, copiers, scanners, CCTV, and electronic key fobs and cards.

1.5 Misuse of IT and communications systems can damage the business and reputation of the Trust.

1.6 All staff must comply with this policy at all times to protect the Trust's IT and communications systems from unauthorised access, misuse, and harm. Breach of this policy may be dealt with under the Trust's Disciplinary Procedure and, in serious cases, may be treated as gross misconduct leading to summary dismissal.

1.7 In this policy references to personnel/bodies are to the personnel/bodies present within the Trust, or other Trust site at which the particular member of staff reviewing the policy is engaged.

2 Who is Covered by the Policy?

2.1 This policy covers all individuals working at all levels and grades, including senior managers, officers, directors, employees, consultants, contractors, trainees, homeworkers, part-time and fixed-term employees, casual and agency staff and volunteers (collectively referred to as staff for the purposes of this policy).

2.2 Third parties who have access to the Trust's IT and communication systems are also required to comply with this policy.

3 Who is Responsible for this Policy?

3.1 The Trust has overall responsibility for the effective operation of this policy, but has delegated day-to-day responsibility for its operation to the Headteacher.

3.2 The IT Technician will deal with requests for permission or assistance under any provisions of this policy, subject to their primary tasks of maintaining the Trust's core systems, and may specify certain standards of equipment or procedures to ensure security and compatibility.

3.3 The Senior Leadership Team and all other management have a specific responsibility to operate within the boundaries of this policy, ensure that all staff understand the standards of behaviour expected of them and to take action when behaviour falls below its requirements.

3.4 All staff are responsible for the success of this policy and should ensure that they take the time to read and understand it. Any misuse of our electronic communications systems or equipment should be reported to the

Headteacher. Questions regarding the content or application of this policy should be directed to the Headteacher or the Senior Leadership Team.

4 Equipment Security and Passwords

4.1 Staff are responsible for the security of the equipment allocated to or used by them, and they must not allow it to be used by anyone other than in accordance with this policy.

4.2 If given access to the e-mail system or to the internet, staff are responsible for the security terminals and devices. If leaving a terminal or device unattended or on leaving the office/classroom staff must ensure that the terminal or device is locked or they have logged off to prevent unauthorised users accessing the system in their absence. Staff without authorisation should only be allowed to use terminals under supervision.

4.3 Desktop PCs and cabling for telephones or computer equipment should not be moved or tampered with without first consulting the IT Technician.

4.4 Passwords are unique to each user and must be changed regularly to ensure confidentiality. Passwords must be kept confidential and must not be made available to anyone else unless authorised by the Headteacher. Staff must not use another person's username and password or allow anyone else to log on using their personal username and password. On the termination of employment or engagement (for any reason) all members of staff will be required to provide details of their passwords to the Headteacher and return any equipment, key fobs or cards.

4.5 Staff who have been issued with a laptop, tablet, PDA or mobile telephones must ensure that it is kept secure at all times, especially when travelling. Appropriate steps, including the use of passwords, must be taken to secure access to data kept on such equipment to ensure that confidential data is protected in the event of loss or theft. Staff should also be aware that when using equipment away from the workplace, documents may be read by third parties, for example, passengers on public transport.

5 Systems and Date Security

5.1 Staff should not delete, destroy or modify existing systems, programs, information or data which could have the effect of harming the Trust or exposing it to risk (except as authorised in the proper performance of their duties).

5.2 Staff should not download or install software from external sources. Downloading unauthorised software may interfere with the Trust's systems and may introduce viruses or other malware. This includes software programs, instant messaging programs, screensavers, photos, video clips, music or similar files. Incoming files and data should always be virus-checked before they are downloaded. If in doubt, staff should seek advice from the IT Technician.

5.3 Staff must not attach any device or equipment to the Trust's systems without the prior approval of the IT Technician. This includes any USB storage devices, mobile phones, tablet computers or PDA. It also includes use of the USB port, infra-red connection port or any other port.

5.4 The Trust monitors all e-mails passing through its system for viruses. Staff should exercise particular caution when opening e-mails from unknown external sources or where, for any reason, an e-mail appears suspicious (for example, if its name ends in .ex). The IT Technician should be informed immediately if a suspected virus is received. The Trust reserves the right to block access to attachments to e-mails for the purpose of effective

use of the system and for compliance with this policy. The Trust also reserves the right not to transmit any e-mail message.

5.5 Staff must not attempt to gain access to restricted areas of the network, or to any password-protected information, unless specifically authorised.

5.6 When using laptops, tablets or other Wi-Fi enabled equipment staff must be particularly vigilant about its use outside the office and take any precautions required by the IT Technician from time to time against importing viruses or compromising the security of the system. The system contains information which is confidential to the Trust's business and/or which is subject to data protection legislation. Such information must be treated with extreme care and in accordance with the Trust's Data Protection Policy.

6 E-mail Etiquette and Content

6.1 E-mail is a vital tool, but an informal means of communication, and should be used with great care and discipline. Staff should always consider if e-mail is the appropriate method for a particular communication. Correspondence with third parties by e-mail should be written as professionally as a letter. Messages should be concise and directed only to relevant individuals.

6.2 Staff must not send abusive, obscene, discriminatory, extremist, racist, sexist, Islamophobic, anti-Semitic, homophobic, harassing racist, harassing, derogatory, defamatory, or otherwise inappropriate e-mails. Anyone who feels that they have been harassed or bullied, or are offended by material received from a colleague via e-mail should inform the Senior Leadership Team or the Headteacher.

6.3 Staff should take care with the content of e-mail messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract. Staff should assume that e-mail messages may be read by others and not include anything which would offend or embarrass any reader, or themselves, if it found its way into the public domain.

6.4 E-mail messages may be disclosed in legal proceedings in the same way as paper documents. Deletion from a user's inbox or archives does not mean that an e-mail cannot be recovered for the purposes of disclosure. All e-mail messages should be treated as potentially retrievable, either from the main server or using specialist software.

6.5 In general, staff should not:

6.5.1 send or forward private e-mails at work which they would not want a third party to read;

6.5.2 send or forward chain mail, junk mail, cartoons, jokes or gossip;

6.5.3 contribute to system congestion by sending trivial messages or unnecessarily copying or forwarding e-mails to those who do not have a real need to receive them;

6.5.4 agree to terms, enter into contractual commitments or make representations by e-mail unless appropriate authority has been obtained. A name typed at the end of an e-mail is a signature in the same way as a name written at the end of a letter;

6.5.5 download or e-mail text, music and other content on the internet subject to copyright protection, unless it is clear that the owner of such works allows this;

6.5.6 send messages from another person's computer or email address or under an assumed name unless specifically authorised; or

6.5.7 send confidential messages via e-mail or the internet, or by other means of external communication which are known not to be secure.

6.6 Staff should return any wrongly-delivered e-mail received to the sender.

7 Use of the Internet

7.1 When a website is visited, devices such as cookies, tags or web beacons may be employed to enable the site owner to identify and monitor visitors. If the website is of a kind described in paragraph 10.2, such a marker could be a source of embarrassment to the visitor and the Trust, especially if inappropriate material has been accessed, downloaded, stored or forwarded from the website. Such actions may also, in certain circumstances, amount to a criminal offence if, for example, the material is pornographic in nature or suggests links to extremism or terrorism. This is further considered at paragraph 10.

7.2 Staff should not access any web page or download any files (whether documents, images or other) downloaded from the internet which could, in any way, be regarded as illegal, offensive, in bad taste or immoral. While content may be legal in the UK, it may be in sufficient bad taste to fall within this prohibition. As a general rule, if any person (whether intended to view the page or not) might be offended by the contents of a page, or if the fact that our software has accessed the page or file might be a source of embarrassment or offence if made public, then viewing it will be a breach of this policy.

7.3 Staff should not under any circumstances use the Trust's systems to participate in any internet chat room, post messages on any internet message board or set up or log text or information on a blog or wiki, even in their own time.

8 Personal Use of Systems

8.1 The Trust permits the incidental use of internet, e-mail and telephone systems to send personal e-mail, browse the internet and make personal telephone calls subject to certain conditions set out below. Personal use is a privilege and not a right. It must be neither abused nor overused and the Trust reserves the right to withdraw its permission at any time or restrict access at its discretion.

8.2 Personal use must meet the following conditions:

8.2.1 use must be minimal and take place substantially out of normal working hours (that is, during lunch hours, before 9 am or after 4 pm);

8.2.2 personal e-mails must be labelled personal in the subject header;

8.2.3 use must not interfere with school or office commitments;

8.2.4 use must not commit the Trust to any marginal costs; and

8.2.5 use must comply with the Trust's policies including the Social Media, Equal Opportunities and Anti-Harassment Policy, Data Protection Policy, Code of Conduct and Disciplinary Procedure.

8.3 Staff should be aware that personal use of the Trust's systems may be monitored and, where breaches of this policy are found, action may be taken under the Trust's Disciplinary Policy. The Trust reserves the right to restrict or prevent access to certain telephone numbers or internet sites if personal use is considered to be excessive.

9 Monitoring of Use of Systems

9.1 The Trust's systems enable the Trust to monitor telephone, e-mail, voicemail, internet and other communications. For business reasons, and in order to carry out legal obligations in the Trust's role as an employer, use of the Trust's systems including the telephone and computer systems, and any personal use of them, is continually monitored. Monitoring is only carried out to the extent permitted or as required by law and as necessary and justifiable for business purposes.

9.2 More particularly staff should be aware that the Trust has appropriate systems in place to monitor and filter email and internet use on its systems in order to comply with its obligations under the Prevent Duty. The Prevent Duty is aimed at ensuring pupils are protected from terrorist and extremist materials and staff should be aware that if they are found deliberately accessing internet sites, social media forums or groups containing extremist, incitements to violence or terrorist materials will be subject to disciplinary action.

9.3 A CCTV system monitors the exterior of the building 24 hours a day. This data is recorded.

9.4 The Trust reserves the right to retrieve the contents of e-mail messages or check internet usage (including pages visited and searches made) as reasonably necessary in the interests of the Trust, including the following purposes (this list is not exhaustive):

9.4.1 to monitor whether the use of the e-mail system or the internet is legitimate and in accordance with this policy;

9.4.2 to find lost messages or to retrieve messages lost due to computer failure;

9.4.3 to assist in the investigation of alleged wrongdoing; or

9.4.4 to comply with any legal obligation.

10 Prohibited Use of Equipment and Systems

10.1 Access is granted to the internet, telephones and other electronic systems for legitimate business purposes only. Incidental personal use is permissible provided it is in full compliance with the Trust's rules, policies and procedures (including this policy, the Social Media, Equal Opportunities, Anti-harassment and Bullying Policy, Data Protection Policy and Disciplinary Policy).

10.2 Misuse or excessive personal use or abuse of the Trust's telephone or e-mail system, or inappropriate use of the internet in breach of this policy will be dealt with under the Trust's Disciplinary Policy. Misuse of the internet can, in certain circumstances, constitute a criminal offence. In particular, misuse of the e-mail system or inappropriate use of the internet by participating in online gambling or chain letters or by creating, viewing, accessing, transmitting or downloading any of the following material will amount to gross misconduct (this list is not exhaustive):

10.2.1 pornographic material (that is, writing, pictures, films and video clips of a sexually explicit or arousing nature);

10.2.2 material that is extremist, terrorist or amounts to incitements to violence;

10.2.3 offensive, obscene, or criminal material or material which is liable to cause embarrassment or damage the reputation of the Trust;

10.2.4 a false and defamatory statement about any person or organisation;

10.2.5 material which is discriminatory, offensive, derogatory or may cause embarrassment to others (including material which breaches the Trust's Equal Opportunities or Anti-harassment and Bullying Policy);

10.2.6 confidential information about the Trust or any of the Trust's staff, pupils or parents (including that which a member of staff does not have authority to access);

10.2.7 any other statement which is likely to create any liability (whether criminal or civil, and whether for the individual member of staff or the Trust); or

10.2.8 material in breach of copyright.

Any such action will be treated very seriously and is likely to result in summary dismissal.

10.3 Where evidence of misuse is found in respect of a more detailed investigation may be undertaken in accordance with the Trust's Disciplinary Procedure, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or managers involved in the Disciplinary Procedure. If necessary, such information may be handed to the police in connection with a criminal investigation and/or provided to the Local Safeguarding Officer or other officer or body as appropriate in the circumstances.

10.4 Where evidence of misuse is found in respect of staff who are not employees of the Trust action may be taken in line with the nature of that relationship and may include a more detailed investigation involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or managers involved. If necessary, such information may be handed to the police in connection with a criminal investigation and/or provided to the Local Safeguarding Officer or other officer or body as appropriate in the circumstances.

Approved by: _____ _____

Chair of Trust **CEO**

Date: _____ _____